2. (Amended) The method of claim 1, further comprising, before passing the encrypted network [packets] packet to the computer on the [internal] network that is internal with respect to the first computer

determining a destination computer for the [each] encrypted network packet.

B1 cont'd

3. (Amended) The method of claim 2, wherein determining a destination computer further includes:

determining whether a source computer that sent the [each] encrypted network packet is authorized to send encrypted network packets to the destination computer.

4. (Amended) The method of claim 2, wherein determining a destination computer includes:

examining [a field] an index field in a header of the network packet.

B2

6. (Amended) The method of claim 2, wherein an encrypted network packet is passed to the computer on the [internal] network that is internal with respect to the first computer when the destination computer for the encrypted network packet is determined to be the computer on the [internal] network that is internal with respect to the first computer.

22

7. (Amended) The method of claim 1, further comprising:

decrypting an encrypted network packet at the [network interface] first computer when the destination computer for the encrypted network packet is determined to be the [network interface] first computer.

B2 cont

8. (Amended) The method of claim 7, further comprising:

passing the decrypted network packet to the computer on the [internal] network that is internal with respect to the first computer.

9. (Amended) The method of claim 1, further comprising:

encrypting network packets; and

sending encrypted network packets from the [network interface] first computer to the external network.

10. (Amended) The method of claim 9, wherein the computer on the [internal] network that is internal with respect to the first computer encrypts the network packets, and further comprising:

passing the encrypted network packets to the [network interface] first computer.

B2 cont

11. (Amended) The method of claim 1, wherein the [network interface] first computer comprises a firewall computer.

12. (Amended) The method of claim 1, wherein the external network comprises a public network.

Cancel claim 13 without prejudice.

B3

14. (Amended) [The method of claim 13] A method of handling a network packet, [further] comprising

receiving an encrypted network packet at a first computer over a network from a source computer;

examining a [the] field in the network packet to determine which of a plurality of encryption algorithms was used to encrypt the network packet and to determine a destination computer for each encrypted network packet[.] ; and

decrypting the network packet at the determined destination computer.

B4

19. (Amended) The method of claim [13] 14, wherein the field corresponds to a virtual network tunnel.

20. (Amended) The method of claim [13] 14, wherein the network comprises a public network.

24

21. (Amended) The method of claim [13] 14, wherein the first computer comprises a firewall computer.

B4

22. (Amended) A method of handling an encrypted network packet [packets], comprising:

receiving the encrypted network packet [packets] sent over a network at a first computer;

determining which virtual tunnel the [each] network packet was sent over; and

routing the [each] network packet to a destination computer that is internal with respect to the first computer in accordance with the determined virtual tunnel.

B5

24. (Amended) A method of handling a network packet [packets], comprising:

encrypting network packets at a first computer connected to an internal network;

storing a virtual tunnel identifier in the packet that is used to determine routing of the packet;

passing the encrypted network packet over the internal network to a public network interface computer; and

passing the encrypted network packet over a public network connected to the public network interface computer.

25. (Amended) A method of handling network packets, comprising:

28

receiving network packets sent over a network at a first computer;

B5 cont

examining each packet's virtual tunnel field to determine [determining] which virtual tunnel each network packet was sent over [;] and whether a source computer that sent each network packet is authorized to send network packets over the determined virtual tunnel.

[determining whether a source computer that sent each network packet is authorized to send network packets [to] over the determined virtual tunnel.]

Add the following new claim:

~~27~~ 13 ~~28~~. A method of handling network packets, comprising

B6

receiving an encrypted network packet from a public network at a firewall computer;

determining the destination computer of the encrypted network packet by examining a virtual tunnel field that corresponds to the method of encryption;

determining whether a source computer that sent the encrypted network packet is authorized to send encrypted network packets to the destination computer; and

determining whether to decrypt the encrypted network packet at the firewall computer or to pass the encrypted network packet to a computer on a network that is internal with respect to the first computer for decryption.--